Great Game Huddle Notes
August 13, 2019

Mark and Skylar from Information Systems welcomed everyone to the Huddle.

To begin the presentation on Cyber Security, they asked a question:
"Why are we in the line of fire?"

It is because information = $$$. What does that mean?
- Nothing is free. There is always going to be a cost.
- A cost of giving your email out to a free website that gives you fun music for a presentation. (Royalty Free Music Studio)
- An email address is enough information for someone to make $$$.
- By signing/giving your email address you are agreeing to let someone get your address, phone number, etc.

Remember:
> **Anything** or **Anyone** that connects to the internet is possible target.
> (Microsoft, Apple, Android)

Types of Attack
- Targeted - A hacker can target any company they do not like for any reason and it is harder for IT to defend against.
- Opportunistic - A hacker is not deliberately targeting an individual or organization. They want to see who will fall into their net and IT will be able to defend an attack

Public Sector
Public sector ransomware attacks are trending up - 53 known attacks in 2018 and 21 known public-sector attacks as of April.

Ransomware:
- $338,700 is the average paid for public section, however, it cost more to rebuild the system.
- A quick review of the organization's website can give a snapshot of their ability to pay.
  - Example: Reviewing the transparency portal or the financial huddle pages can demonstrate we have money in reserve – a hacker may request 1 or 2%.
- Cost of data breech may equal up $2.3 million, plus the cost of protection on the individual credit.

Fun Facts:
- IS blocked an average of 1400 Malicious connections and intrusion attempts **every** day.
- Leadership are targets because information is on the public website.
- 90% of breaches involve phishing.

Recent Incidents:
- Social Engineering: compromised County account to order hardware
- Social Engineering: fake tech support call; remote access
- Social Engineering: Payroll attack
- Compromised accounts: Typically data breeches elsewhere